

Wasabi + Veeam: The Most Resilient, Cost-Predictable Data Protection Solution

TL: DR: Veeam Data Platform brings AI-driven backup, recovery, and threat detection; Wasabi brings immutable, No egress or API fees hot cloud storage. Together, they give organizations a faster, more secure, cost-predictable path to 3-2-1-1-0 best practices and clean ransomware recovery without surprise storage bills.

Wasabi + Veeam: Built for the AI Era of Data Resilience

Data keeps growing faster than budgets, and expectations have grown with it: faster recovery SLAs, AI-assisted threat detection, and audit-ready compliance are now baseline requirements. Veeam Data Platform unifies backup, recovery, security, and compliance across virtual, physical, cloud, and SaaS workloads, with Veeam Intelligence, its AI-driven layer, surfacing risks, recommending clean recovery points, and automating threat detection. Wasabi extends that platform with secure, immutable hot cloud storage priced predictably, with no egress or API fees, so backup, DR testing, and ransomware recovery never come with a surprise bill.

How Do Wasabi and Veeam Protect Against Ransomware?

Veeam's AI-powered malware and anomaly detection, threat scanning, and instant recovery validate that a restore point is clean before you recover it. Wasabi adds an air-gapped, immutable layer underneath: Object Lock ensures backups written to Wasabi cannot be deleted or altered, for as long as your retention policy requires.

Wasabi Multi-User Authorization removes single-administrator control over protected, high-impact actions by requiring approval from every security contact assigned to the activity before the action can proceed. Veeam Four-Eyes Authorization adds another layer of separation of duties within the backup environment, requiring a second authorized user to approve sensitive operations such as deleting backups or snapshots, removing repositories, managing users, or changing MFA settings. Together, Wasabi and Veeam protect both the storage and backup control planes, reducing the risk that one compromised credential, rogue administrator, or AI-assisted attack can destroy critical recovery options. These layered controls strengthen the immutable-copy and operational-resilience objectives of a 3-2-1-1-0 data-protection strategy.

Features

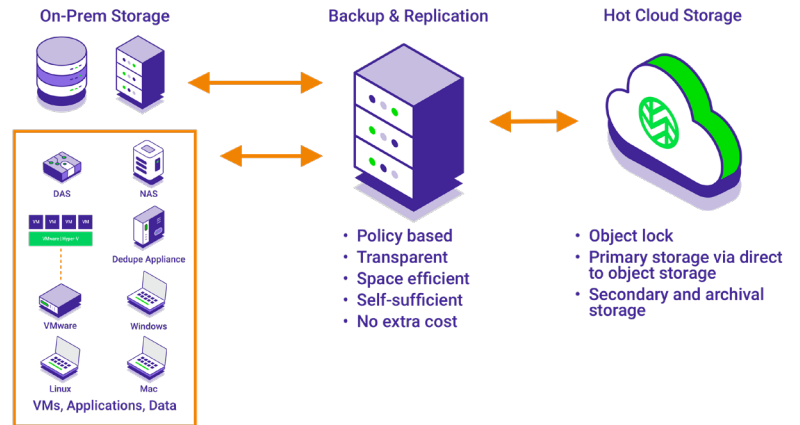
- Affordable, predictable off-site and cloud-native backup copies
- Seamless integration with Veeam Data Platform, including direct-to-object and SOBR
- Secure, immutable cloud copies via Object Lock
- No added cost to extend secure locks (API) or restore backups (egress)

Benefits

- Cyber-resilient data protection, reinforced by Veeam's AI-driven threat detection
- Predictable cost with no hidden egress, API, or retrieval fees
- Confidence in the authenticity and availability of every backup copy
- Simplified compliance with the 3-2-1-1-0 rule and audit-ready reporting

What Is Direct-to-Object Backup with Wasabi and Veeam?

Veeam supports direct-to-object backup, letting you write straight to Wasabi as a repository, with no on-prem staging required. This lowers the cost and complexity of backup infrastructure while providing distributed environments with a single, centralized cloud repository.



Why Is Wasabi a Lower-Cost Cloud Storage Option for Veeam?

Wasabi charges no fees for egress or API calls, and the price doesn't change based on how often data is accessed; it is a flat rate, whether backups sit untouched for months or are restored constantly. That means DR tests, ransomware recovery drills, and real recoveries can happen as often as needed without a variable bill, and disaster recovery plans can be validated freely instead of being budgeted around hidden costs.

How Does Wasabi Strengthen Veeam Data Platform Deployments?

Wasabi is built to be the cloud object-storage for Veeam Data Platform. It works as a capacity tier or as a direct repository for any workload Veeam protects, provides a flat, predictable cost for every backup, regardless of how often it's accessed, and adds an immutable, air-gapped copy that stands apart from the production environment. For teams standardizing on Veeam, that combination turns cloud storage from a variable line item into a fixed, predictably budgeted part of the data protection strategy.

Frequently Asked Questions

Does Wasabi charge egress fees when used with Veeam Data Platform?

No. Wasabi does not charge egress or API fees, so restoring backups, running DR tests, or migrating data out of Wasabi costs the same as storing it.

Can Wasabi serve as a Veeam Scale-out Backup Repository (SOBR)?

Yes. Wasabi integrates as a capacity tier or repository extent within Veeam Data Platform, including direct-to-object backup from Veeam servers and Veeam Agents.

Is data stored in Wasabi immutable?

Yes. Wasabi supports Object Lock, which prevents backups from being deleted or altered for the length of the retention period, even by an attacker with valid credentials, and pairs with Wasabi MUA and Veeam Four-Eyes Authorization for layered protection.

Does Wasabi support Veeam direct-to-object backup?

Yes. Veeam can send backups directly to Wasabi, including NAS and endpoint backups.

Learn more at wasabi.com/Veeam